KLJN STATISTICAL PHYSICAL SECURE KEY EXCHANGE SYSTEM: ATTACKS AND DEFENSE

A Dissertation

by

HSIEN-PU CHEN

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Laszlo B. Kish
Committee Members,	Jun Zou
	Peng Li
	Andreas Klappenecker
Head of Department,	Miroslav Begovic

May 2016

Major Subject: Electrical Engineering

ABSTRACT

The Kirchhoff-law-Johnson-noise (KLJN) scheme is a statistical/physical secure key exchange system based on the laws of classical statistical physics to provide unconditional security. This dissertation contains three main studies of the KLJN system.

The first study presents the refutation of a physical model, proposed by Gunn, Allison and Abbott (GAA), to utilize electromagnetic waves for eavesdropping on the KLJN secure key distribution. The correct mathematical model of the GAA scheme is deduced, which is based on impedances at the quasi-static limit. Mathematical analysis and simulation results confirm our approach and prove that GAA's experimental interpretation is incorrect too.

The second study analyzes one of the passive (listening) attacks against the KLJN system, the cable capacitance attack. In practical situations, due to the non-idealities of the building elements, there is a small information leak, which can be mitigated by privacy amplification or other techniques so that unconditional (information-theoretic) security is preserved. The industrial cable and circuit simulator LTSPICE is used to validate the information leak due to one of the non-idealities in KLJN, the parasitic (cable) capacitance. Simulation results show that privacy amplification and/or capacitor killer (capacitance compensation) arrangements can effectively eliminate the leak.

The third study explores one of the major active (invasive) attacks, the current injection attack. The LTSPICE is used to emulate the attack against the ideal and a

practical KLJN system, respectively. It is shown that two security enhancement techniques, namely, the instantaneous voltage/current comparison method, and a simple privacy amplification scheme, independently and effectively eliminate the information leak and successfully preserve the system's unconditional security.

To my family

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Laszlo B. Kish, for his guidance and great support throughout the course of my research at Texas A&M University.

Thanks also go to my committee members Dr. Zou, Dr. Li, and Dr. Klappenecker, for their advice on my research. I thank my friends and the department faculty and staff for making my time at Texas A&M University a great experience.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

1. INTRODUCTION*

1.1 Data Communication Security

Security in data communication is an essential part of today's world. When we connect and communicate via the Internet, we expect the data communication to be secure. Take the example of the software tools we use to sign in to online banking. Before a secure data exchange can begin, the two communicators (Alice and Bob) must generate and share a joint secret (secure) encryption key through the communication channel, while an eavesdropper (Eve) is supposedly monitoring the related data (see Figure 1).

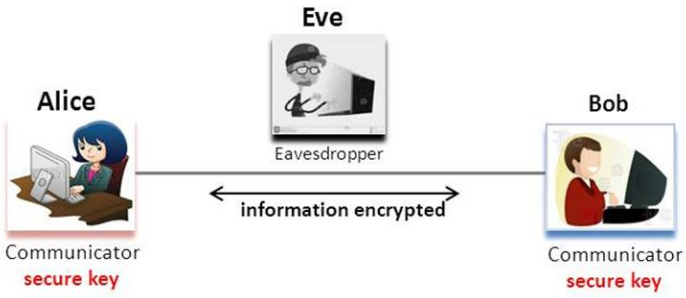

Figure 1 The two communicators (Alice and Bob) must generate and share a joint secure key through the communication channel to encrypt and decrypt their messages, while the eavesdropper (Eve) is monitoring the related data. Software-based methods are only 'computationally safe' and thus potential time bombs [11].

*Part of this section is a modified version of the paper "Current Injection Attack against the KLJN Secure Key Exchange" by H.P. Chen, M. Mohammad, L.B. Kish, which is submitted to the journal *Metrology and Measurement Systems* in Feb 2016 and is pending review.

Software-based tools however can only offer computational security (or conditional security), which is not a future-proof security. The extraction of the keys is limited only by Eve's computational resources. If Eve had a sufficiently fast computer with standard algorithms or a genuinely powerful algorithm, she could extract the secure key and decrypt the communicated data with reasonable speed in the future. With computing solutions progressing at a high pace, existing software-based secure communication is a potential time bomb.

1.2 Unconditionally Secure Key Exchange

Therefore, scientists have been working on physics-based secure key exchange schemes which are unconditionally secure. Unconditional security (or *information theoretic security*) means that, even in the case of a perfectly able eavesdropper, the perfect security limit (zero information for Eve) of communication can be approached if sufficient resources (time, etc.) are available [1].

It is essential in intelligent vehicle systems [2,3]; for power and sensor networks of strategical importance [4,5]; for ultra-strong PUF hardware keys [6]; and in secure computer, instrument and video game systems [7].

1.2.1 Quantum Key Distribution (QKD)

Quantum key distribution (QKD) is the earliest scheme claimed to be unconditionally secure. It was first proposed by Stephen Wiesner in the 1970s, and later developed by Charles H. Bennett and Gilles Brassard in 1984, and Artur Ekert in 1990 [45-47]. Single photons are used to carry information bits (see Figure 2). In this scheme, the security is based on the 'no-cloning-theorem' of quantum physics [48]. The idea is that a single photon cannot be copied without noise (error). The photon gets destroyed when Eve captures and measures it. She has to re-generate and re-inject it into the channel, otherwise Alice and Bob will consider the bit invalid. However, when Eve restores the photon, due to the no-cloning rule, noise is introduced. Thus the error rate in the channel will be greater than without eavesdropping. Alice and Bob will discover the eavesdropping after analyzing a number of transmitted bits and their errors [11].

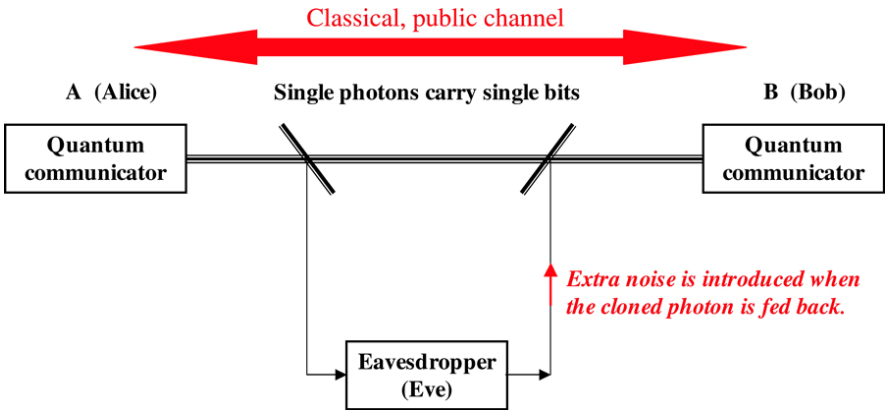

Figure 2 Generic quantum communication arrangement. Detecting the eavesdropper requires the statistics of bit errors, which calls for a sufficiently large number of bits. The communication of only a few bits is not secure [11].

In due course, QKD's fundamental security claims have been debated by experts in the field [49-55]. Furthermore, its practical realizations, including all commercial quantum communicators, have been fully cracked. These attacks have been done by hacking, that is, by utilizing non-ideal features of the hardware components [56-69]. Note, counter-measures (patches) were later proposed to overcome these attacks. However, before these patches were invented, the eavesdroppers could have fully utilized such attacks [70-73]; which means these systems had not offered any unconditional security, at all. The security was only conditional and the condition was that Eve avoided these attacks.

1.2.2 The Kirchhoff-law-Johnson-noise (KLJN) Secure Key Exchange Scheme

It was a commonly accepted assumption for years that only QKD would be able to perform unconditionally secure key exchange. However, this dogma was refuted in 2005 when Laszlo B. Kish introduced the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange scheme [9], which was subsequently experimentally demonstrated [17]. The KLJN scheme is the only classical physical competitor of quantum communicators [1]. Its security is based on the Fluctuation-Dissipation Theorem [9] of classical statistical physics and the properties of Gaussian stochastic processes [12]. Currently, it is also the only unconditionally secure key exchange that can be integrated on a chip and has reasonable price [8-11] .

The core KLJN secure key exchange system [1,9-11,32-40] is shown in Figure 3, while [2-7] and [41-43] are dealing with advanced aspects with expansions and applications.

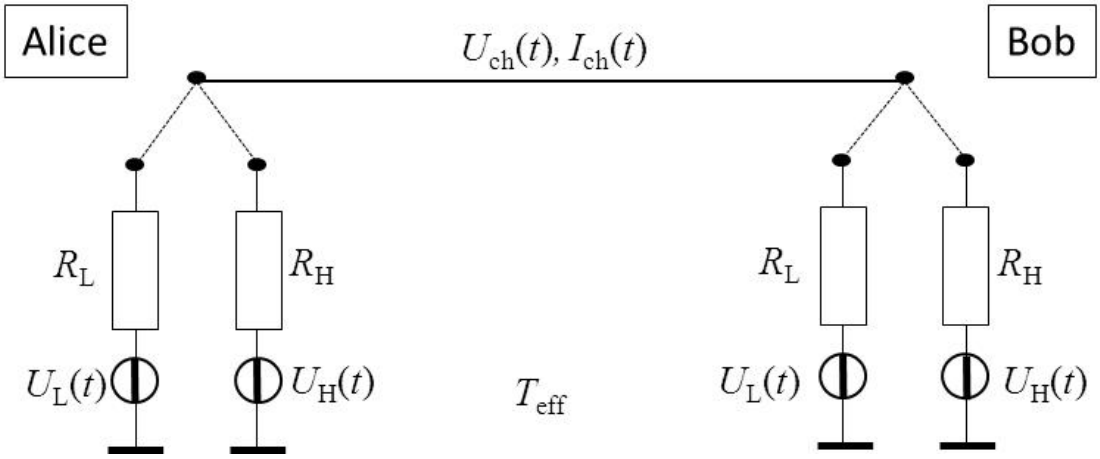

Figure 3 Schematics of the Kirchhoff-law-Johnson-(like)-noise (KLJN) secure key exchange system. The resistor values are R_L and R_H. The thermal noise voltages, $U_L(t)$ and $U_H(t)$, are generated at an effective temperature, T_{eff}. The channel noise voltage and current are $U_{ch}(t)$ and $I_{ch}(t)$, respectively [13].

At the beginning of each bit exchange period (BEP), Alice and Bob, randomly select a resistor from the set $\{R_L, R_H\}$, $R_L \neq R_H$, where R_L represents the Low bit value (L) and R_H the High bit value (H), and they connect the chosen resistors to the wire channel (cable). The Gaussian voltage noise generators emulates the Johnson noise of the resistors and deliver band-limited white noise with publicly agreed bandwidth and temperature, T_{eff}.

Within each BEP, Alice and Bob measure the current and voltage noises, $I_{\mathrm{ch}}(t)$ and $U_{\mathrm{ch}}(t)$, in the cable. Using the Johnson formula, they derive the unknown resistance value at the other end of the cable which is the difference between their own resistance and the total loop resistance [9]. Though Eve can also obtain the total loop resistance, she cannot distinguish the LH and HL bit situations, which indicates a secure bit exchange. The HH and LL bit situations are disregarded.

1.3 Brief Literature Review - Attacks and Defense of KLJN Secure Key Exchange Scheme

There have been various valid attacks causing some information leak but not a full crack, such as methods using the cable capacitance [13], cable resistance (Bergou-Scheuer-Yariv attack) [14-18], temperature-inaccuracy (Hao-attack) [19-21]. However, in each case, the information leak can be eliminated whenever sufficient resources (either specific hardware, higher accuracy, or enough time for privacy amplification) are available, thus the system stays unconditionally secure [1].

Some other attacks are only unsuccessful attempts with fundamental flaws in their model and physics; perhaps the best example the Gunn-Allison-Abbott (GAA) "directional coupler" attack [22], where conceptual and theoretical flaws [23-25] suggest that a directional coupler can be built and that will serve with information leak. However, directional coupler cannot be built for the KLJN's no-wave (quasi static) situation. Moreover, it could not cause information leak even if existed [23-25]. Most interestingly

are the experimental errors in [22], (see them rebutted in [26]), which seemingly support the unjustified expectations.

Another one, a high-profile many-sided cracking attempt by Bennett-Riedel [27] has also failed with all of its goals, see [28], further indicating that physical security is a subtle topic. We also mention an earlier unsuccessful attempt [29], which, similarly to the above ones, triggered discussions [30] with valuable outcomes. Finally, we mention a recent transient attack by GAA [31], which is valid even though there are serious flaws both in the security and physics aspect of the paper, and a simple solution does exist [32] to fully eliminate this attack, too.

In conclusion, the unconditional security of the KLJN scheme remains unchallenged. As with the evolution of quantum communicators, further attacks schemes are expected to emerge and to trigger new defense solutions that nullify those attacks, too.

1.4 Dissertation Focus

This dissertation focuses primarily on the attacks and defense of the practical KLJN secure key exchange scheme.

The first study is regarding a physical model proposed by Gunn, Allison and Abbott (GAA) [22] who proposed a new, delay-based attack against the KLJN secure key exchange scheme [1,28,33,44] in 2014. In the study, this model is refuted and subsequently a correct mathematical model of the scheme based on impedances at the

quasi-static limit is deduced. Mathematical analysis and simulation results confirm our approach and prove that GAA's experimental interpretation is incorrect too.

The second study analyzes one of the passive (listening) attacks against the KLJN system, the cable capacitance attack. Similarly to quantum key distribution, in practical situations, due to the non-idealities of the building elements, there is a small information leak, which can be mitigated by privacy amplification or other techniques so that unconditional (information-theoretic) security is preserved. In the study, the industrial cable and circuit simulator LTSPICE is used to validate the information leak due to one of the non-idealities in KLJN, the parasitic (cable) capacitance. Simulation results show that privacy amplification and/or capacitor killer (capacitance compensation) arrangements can effectively eliminate the leak.

The third study explores one of the major active (invasive) attacks, the current injection attack. The LTSPICE is used to emulate the attack against the ideal and a practical KLJN system, respectively. It is shown that two security enhancement techniques, namely, the instantaneous voltage/current comparison method, and a simple privacy amplification scheme, independently and effectively eliminate the information leak and successfully preserve the system's unconditional security.

Conclusion is presented at the end to summarize the key points drawn from the studies.

2. ELECTROMAGNETIC WAVES DO NOT EXIST IN A SHORT CABLE AT LOW FREQUENCIES*

2.1 Introduction

The study in this section is also included in the paper "Do Electromagnetic Waves Exist in a Short Cable at Low Frequencies? What does Physics Say?" [23]. The paper was accepted and published by the journal *Fluctuation and Noise Letters* in 2014.

In 2014, Gunn, Allison and Abbott (GAA) [22] proposed a physical model to utilize electromagnetic waves for eavesdropping on the KLJN secure key distribution [1,28,33,44]. Their model, and its theoretical underpinnings, is found to be fundamentally flawed [23] because their assumption of electromagnetic waves violates the wave equation.

First we provide an overview of GAA's claim, followed by our refutation of their proposed physical model and their experimental interpretations. After that we present a correct mathematical model of the scheme. Then, simulation results are shown which can also confirm our approach and prove that GAA's experimental explanation is incorrect.

---

*Reprinted with permission from "Do Electromagnetic Waves Exist in a Short Cable at Low Frequencies? What does Physics Say?" by H.P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera, 2014. *Fluctuation and Noise Letters*, 13, 1450016, © [2014] by World Scientific Publishing Company.

2.2 GAA's Claim – Waves Exist in a Finite-Size Cable at Arbitrarily Low Frequencies

A new, delay-based attack against the KLJN secure key distribution scheme [1,28,33,44] is proposed by Gunn, Allison and Abbott (GAA) [22] in 2014. GAA claim—contradicting earlier statements most recently expounded in work by Kish, Abbott and Granqvist (KAG) [28]—that waves exist in a *finite-size* cable at *arbitrarily low frequencies*.

The theoretical basis of GAA's assertion [22] is the fact that, whereas wave-guides usually have a low-frequency cut-off for wave modes versus the *diameter* of the wave-guide, no such cut-off exists for transversal electromagnetic (TEM) wave modes in the case of *infinitely* long wave-guides. GAA write that, because coaxial cables have TEM wave modes, there is no frequency cut-off of the wave-based component of the electrical transport down to zero frequency. As a consequence of their presumption, GAA use the d'Alembert solution [22]

$$U(t,x) = U_{+}\left(t - \frac{x}{v}\right) + U_{-}\left(t - \frac{x}{v}\right) \tag{1}$$

for propagating lossless fluctuations—which may or may not be waves—in a linear medium to model the propagation of voltage in the cable used for key exchange in the KLJN scheme, where U_+ and U_- are voltage components of waves propagating to the

right and left along the x axis, and v is propagation velocity.

The experimental support of GAA's claim is that they have measured the voltage between the ends of a short coaxial cable at low-frequency sinusoidal voltage drive with an impedance-matched load at the other end and, at first sight, have found that their results confirmed some of the implications of Eq. 1, as further elaborated in Section 2.5 below.

We have analyzed GAA's statements [22] and found most of them invalid. Specifically, our findings and conclusions are the following:

(i) In cables, wave modes with wavelengths greater than twice their length are forbidden states, meaning that such modes do not exist; consequently there are no waves in cables in the frequency range pertinent to the KLJN scheme.

(ii) Instead, time-dependent propagation processes are non-wave type retarded potentials in a distributed impedance system; one of the implications of this is that Eq. 1 does not hold.

(iii) GAA's interpretation of their own "wave-verification" experiments [22] is invalid.

2.3 Refutation of GAA's Theory and Experimental Interpretation

As mentioned above, GAA's attack [22] on the KLJN scheme employs waves and related delays in a cable to extract information. While attempts to utilize time delays in cables for information purposes are to be encouraged, the asserted use of waves,

which do not exist, is a fundamental flaw that invalidates GAA's basic considerations, proposed experiments, and interpretation of these experiments.

The wavelengths corresponding to the frequency range of concern in the KLJN scheme are much longer than the physical extent of the cable, and we earlier referred to that range the "no-wave" or "quasi-static" limit [1,28,33,44]. As remarked above, GAA argue that TEM wave modes do not exhibit any low-frequency cut-off. It is true that TEM wave modes in a wave-guide do not have a low-frequency cut-off versus the diameter of the wave-guide, but this argument is irrelevant because wave modes do have a cut-off versus the length of the cable. This does not imply that the electrical transport itself has a cut-off; it solely means that, when wave modes are forbidden, electrical transport takes place via non-wave phenomena—such as drift and relaxation—which constitute the form of transport in the quasi-static region of electrodynamics.

In this section, we use physics and mathematics to prove that GAA's assumption of the existence of waves in the short cable within the frequency range pertinent to the KLJN scheme violates the wave equation (our proof is given subsequently).

2.4 Violation of the Wave Equation

It was recently pointed out by KAG [28] (including one of the proponents of the GAA model) that the wave equation precludes the existence of waves in the frequency range of concern for the KLNJ scheme. Next we provide more details about this fact and

first illustrate the distributed inductance–capacitance–resistance (LCR) model of the cable in the KLJN scheme in Figure 4.

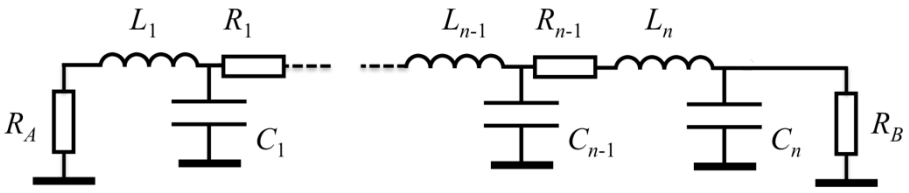

Figure 4 Outline of the pertinent part of the KLJN scheme with a distributed LCR model of a long and leakage-free cable. When the cable losses can be neglected, one may omit the R_i resistors representing the distributed resistance of the cable. Alice's and Bob's resistors, denoted R_A and R_B, respectively, are randomly selected from the set $\{R_L, R_H\}$ with $(R_L \neq R_H)$ at the beginning of each bit-exchange period. These resistors, with associated serial generators (not shown), emulate thermal noise with high noise temperature and strongly limited bandwidth.

For the sake of simplicity but without restricting generality, we discuss the case of a lossless cable. The main conclusion about the lack of wave modes is general because the inclusion of damping terms in harmonic differential equations *can never produce new eigen-frequencies*; they can only modify them and their bandwidth.

The wave equations of voltage $U(x,t)$ and current $I(x,t)$ in lossless cables are

$$\frac{\partial^2 U(x,t)}{\partial x^2} = \frac{1}{v_c^2}\frac{\partial^2 U(x,t)}{\partial t^2}, \tag{2}$$

$$\frac{\partial^2 I(x,t)}{\partial x^2} = \frac{1}{v_c^2}\frac{\partial^2 I(x,t)}{\partial t^2}, \tag{3}$$

where the phase propagation velocity of waves in the cable is

$$v_{\mathrm{c}} = \sqrt{\frac{1}{L_{\mathrm{u}} C_{\mathrm{u}}}} \ . \tag{4}$$

Here L_{u} and C_{u} are inductance and capacitance "densities" of the cable (with units of H/m and F/m), *i.e.*, the unit-length (one-meter) cable inductance and capacitance.

The general classical-physical solutions of these equations in infinite ideal cables are superpositions of waves, with arbitrary frequency, propagating in positive and negative directions in accordance with the d'Alembert solution in Eq. 1. However, in a cable with finite length D, the frequency-space of solutions is quantized to discrete values so that integer multiples of the half-wavelength fit in the cable. Thus the wavelength λ_{max} of the wave with the lowest frequency f_{min} can be written as

$$\lambda_{\mathrm{max}} = 2D \ , \quad f_{\mathrm{min}} = \frac{v_{\mathrm{c}}}{2D} \ . \tag{5}$$

Frequencies below f_{min}, down to zero frequency, constitute a forbidden band of wave states.

The KLJN key exchanger operation strictly requires for security that its frequency range satisfies the quasi-static condition, *i.e.*,

$$f << f_{\min} \ . \tag{6}$$

Thus the wave-based scheme and considerations of GAA for eavesdropping violate not only the wave equations in Eqs. 2 and 3, and its d'Alembert solution in Eq. 1, but also the related other fields of classical and quantum physics of waves, because such non-existent solutions are forbidden states.

We note, in passing, that if the wave-based treatment by GAA [22] were correct, we would not have quantization of atomic electron shells, a forbidden band (energy gap) would not exist in solid state physics, semiconductor devices would not work, and even chemistry would be non-existent or at least very different.

2.5 Correct Treatment of Cable Delays in the Frequency Range for the KLJN Scheme

2.5.1 General Considerations

We showed above that wave modes cannot exist in the cable at the KLJN condition $f << f_{\min}$. A number of questions then arise naturally, such as (*i*) what type of system is the cable under these conditions, (*ii*) what is the nature of the propagating fluctuations caused by Alice's and Bob's noise generators, and (*iii*) are there any other implications of the KLJN condition?

To answer these questions, we first note that the system under consideration is not a waveguide, as implied by GAA [22], but a *distributed impedance network* in the *quasi-static limit*. Secondly, the propagating fluctuations are not waves but phase-shifted voltages and currents; in the language of physics they are related to *retarded potentials* of non-wave solutions, and in electrical engineering vocabulary they are *spatio-temporal fluctuations in an impedance network*.

The general implications of the KLJN conditions are very pervasive, as elaborated and discussed in Section 2.3 & 2.4 above. The specific consequences for the KLJN scheme are that the mathematical and physical framework used by GAA [22] is invalid and that the same applies to their experimental analysis.

When the frequency converges towards zero, the impact of the inductance and capacitance of the cable on the cable current and voltage also rapidly diminish. However, the voltage drop over the cable is determined by its serial resistance R_c and inductance L_c, because the capacitive shunt currents approach zero. Thus the first-order approximation of the cable impedance is

$$Z_c \cong R_c + j2\pi f L_c \ . \tag{7}$$

For simplicity, we analyze the situation wherein the cable loss (resistance) is negligible so that

$$Z_c \cong j2\pi f L_c \ . \tag{8}$$

The corresponding phase delay of the voltage at Bob's end, compared to that of Alice's end, is

$$\varphi_{\mathrm{AB}} = -2\pi f L_{\mathrm{c}} / R_{\mathrm{B}} \tag{9}$$

when the voltage is generated by Alice. This phase delay corresponds to a *frequency-independent time delay* according to

$$\tau_{\mathrm{AB}} = L_{\mathrm{c}} / R_{\mathrm{B}} \quad , \tag{10}$$

which at first glance seems to suggest that we are dealing with waves and that the d'Alembert equation holds, as stated by GAA. However one must realize that this *time delay depends on the load resistance* R_{B} at the other end of the cable, which implies that the *time delay and measured phase velocity in the two directions are different* due to the condition $R_{\mathrm{A}} \neq R_{\mathrm{B}}$ during secure bit exchange [1,28,33,44], *i.e*., under circumstances such that GAA's method [22] is supposed to function. To illustrate this dichotomy, we evaluate the phase delay for voltage propagation in the opposite direction, *i.e*., when the voltage is generated by Bob. Now one finds

$$\varphi_{\mathrm{BA}} = 2\pi f L_{\mathrm{c}} / R_{\mathrm{A}} \tag{11}$$

and

$$\tau_{BA} = L_c / R_A \ . \qquad (12)$$

Thus the d'Alembert equation, applied by GAA [22] to prove the existence of waves, cannot be used in the present situation.

2.5.2 Simulation Based on a Circuit Model for the Cable

To corroborate the theoretical considerations above, we used Linear Technology's LTspice-IV cable simulator software to analyze the experimental situation in GAA's work [22] and confirmed all of their stated results. The simulations proved that a coaxial cable with parameters and conditions similar to those employed by GAA [22] can be modeled with the lumped impedance circuitry shown in Figure 5, where parts (a) and (b) represent a cable with and without loss, respectively.

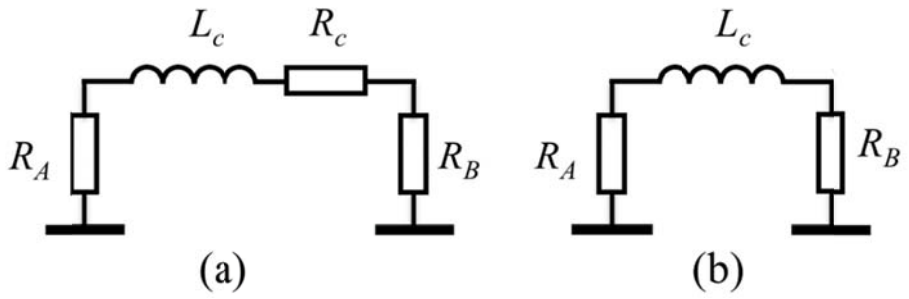

Figure 5 Lumped impedance-components-based model of a cable at low frequencies for analyzing voltage drop along the cable and phase shift in the limit $f << f_{min}$. Part (a) represents a cable with loss (cable inductance and resistance are designated L_c and R_c, respectively), and part (b) represents a lossless cable.

Figure 6 shows results of our simulation addressing the experimental data in GAA's article [22]. The conditions are the same as those of GAA [22] and reported in their Figure 5, but our simulation uses a practical cable model and simple impedance representations (see Figure 5), which fit the cable data to a high degree of accuracy. The practical lossy cable and the simple impedance model in Figure 5a give identical results, while results for the lossless cable (corresponding to data compensated for loss in GAA's work [22]) are nicely represented by the simple inductance model in Figure 5b.

Moreover, it is obvious that the cable inductance L_c produces a voltage drop that is the time-derivative of the current, which is determined predominantly by the resistances in the loop. Thus the voltage drop for the lossless cable is the time derivative of Alice's generator voltage, and this experimental finding by GAA [22] to "support" the d'Alembert equation is simply an inductor-type voltage response and it has nothing to do with waves.

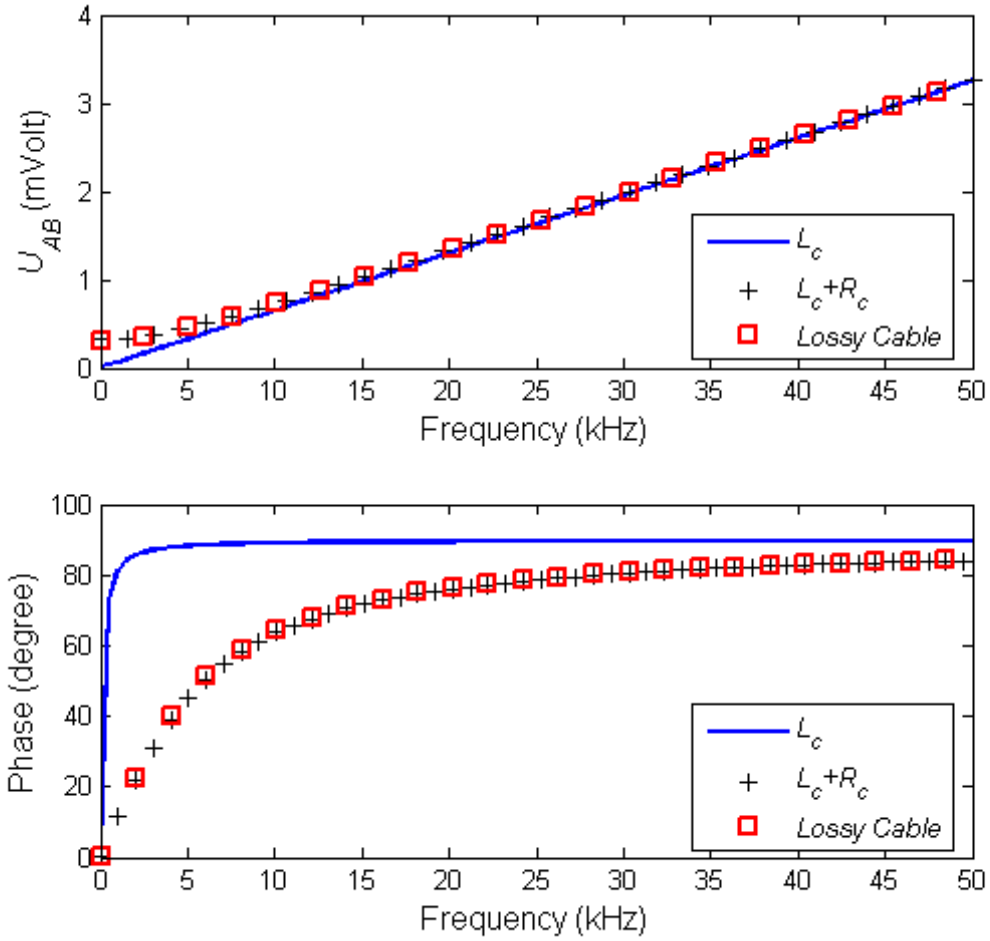

Figure 6 Comparison of simulated data based on impedance models, using LTspice, with those of a real (lossy) cable. Alice's and Bob's resistors, denoted R_A and R_B, have the resistance R_W, and Alice drives the cable with a sinusoidal voltage generator (1 V) via Bob's resistor. The cable is characterized by length D = 1.5 m, L_c = 1.03 μH, R_c = 0.0315 Ω, and C_c = 150 pF. The upper panel shows voltage drop U_{AB} over the cable between Alice's and Bob's ends and the lower panel shows phase shift of U_{AB} compared to that of the voltage at Alice's end. Squares signify simulations of a lossy cable (model RG58), crosses represent data obtained by the use of the lumped-parameters-model in Figure 5a, and the solid line was derived from an inductance model devised to simulate a lossless cable (Figure 5b). These results are in full agreement with the experimental data shown in Figure 5 of GAA's work [22].

To subject Eqs. 10 and 11 to a final test, we evaluated the phase delay and corresponding time delay toward Bob when the resistor at Bob's end was varied and the cable was lossless. Data are shown in Table 1 and verify the correctness of our Eq. 10 to an accuracy of five digits. GAA's "propagation velocity" toward Bob is practically independent of frequency but depends on Bob's resistor. During secure bit exchange, the "propagation" times toward Alice and Bob are different. This fact verifies our conclusion that GAA's use of the d'Alembert equation, as the base of their mathematical considerations, is indeed incorrect.

Table 1 The simulated equivalent phase velocity calculated from phase shifts between the two ends of the cable versus driving frequency and load resistance (the resistance of termination at the other end). The dependence on the resistance is in violation of the d'Alembert equation; for example, in the KLJN system during secure key exchange where the terminal resistances are different. Cable parameters are given in the caption for Figure 6.

	1 kHz	**5 kHz**
10 Ω	3.99998 x 10^7 m/s	4.00018 x 10^7 m/s
20 Ω	7.99996 x 10^7 m/s	8.00038 x 10^7 m/s
50 Ω	1.99999 x 10^8 m/s	2.00007 x 10^8 m/s
1 kΩ	3.99993 x 10^9 m/s	4.00011 x 10^9 m/s
10 kΩ	3.99946 x 10^{10} m/s	4.00041 x 10^{10} m/s

One should observe that, for the cases of 1 kΩ and 10 kΩ, GAA's "phase velocity" is greater than the speed of light. This is acceptable and happens often with the phase velocity of oscillations in a *driven impedance system in the steady-state*; however, it is prohibited in the d'Alembert equation as a consequence of the theory of special

relativity. Similar effects can happen in wave-based systems with reflecting boundary conditions in stationary mode after the waves fill the system; however, in wave-based systems the phase velocity would be the same for the left and right directions.

In conclusion, the proper KLJN scheme is a simple impedance circuitry with related phase shifts where the corresponding time shifts are asymmetrical during secure bit exchange.

3. CABLE CAPACITANCE ATTACK AGAINST THE KLJN SECURE KEY EXCHANGE*

3.1 Introduction

The research in this section is from the paper "Cable Capacitance Attack Against The KLJN Secure Key Exchange" [13], which was submitted to the journal *Information* and was published in 2015.

In the practical KLJN system, due to the non-idealities of the building elements, there is a small information leak. One of such non-idealities is the parasitic cable capacitance of which Eve can exploit to attack the KLJN system. We call it cable capacitance attack. It is a kind of passive (listening) attack, and is also one of the most effective attacks against the practical KLJN system. This attack is first mentioned in 2006 [16], but has never been tested. Subsequently in 2008, a solution was suggested to eliminate this attack by adding a capacitor killer (capacitance compensation) arrangement [17].

In this section, we first present the attack protocol. This is then followed by the simulation of the attack against the practical KLJN system using the industrial cable and circuit simulator LTSPICE by Liner Technology. The information leak and an eavesdropper's success probability in guessing the exchanged key bits are evaluated.

---

*Reprinted with permission from "Cable Capacitance Attack against the KLJN Secure Key Exchange" by H.P. Chen, E. Gonzalez, Y. Saez, L.B. Kish, 2015. *Information*, 6, 719-732, © [2015] by Chen, Gonzalez, Saez and Kish.

Solutions to mitigate this attack, such as the capacitor killer arrangement [17] and privacy amplification [43], are also tested and explained with the simulation results.

3.2 Cable Capacitance Attack

We use coaxial cables because, in this case, the cable capacitance attack [16] can effectively be eliminated without the usage of privacy amplification. However, the attack works with any cable. Coaxial cables include two conductors: the inner wire, which is used as the KLJN channel, and the outer shield, which is grounded (for the ground, see also Figure 7). There is a non-zero capacitance between these two conductors that leads to capacitive currents. Part of the channel noise current is diverted by the parasitic capacitance, which causes a greater current at the end of the lower resistance. This gives Eve a chance to guess the value of the resistors with probability of success greater than 0.5.

Figure 7 shows the distributed elements model of coaxial cables. According to Kirchhoff's current law, at position x, the channel noise current $I_{\mathrm{x}}(t)$ is the sum of the capacitive current $I_{\mathrm{c,x}}(t)$ through the parasitic capacitor element C_{x}, and the channel noise current $I_{\mathrm{x+1}}(t)$. This is written as

$$I_{\mathrm{x}}(t) = I_{\mathrm{c,x}}(t) + I_{\mathrm{x+1}}(t). \tag{13}$$

The capacitive current $I_{c,x}(t)$ is proportional to the time derivative of the channel noise voltage $U_x(t)$ and it is given by

$$I_{c,x}(t) = C_x \cdot \frac{dU_x(t)}{dt}. \tag{14}$$

We define the cross-correlation $\rho(x)$ [28] at position x as the product of the channel noise current and the time derivative of the channel noise voltage:

$$\rho(x) = \left\langle I_x(t) \cdot \frac{dU_x(t)}{dt} \right\rangle_\tau, \tag{15}$$

where $\langle\ \rangle_\tau$ means finite time (τ) average. The location-dependence of $\rho(x)$ represents the information leak [28].

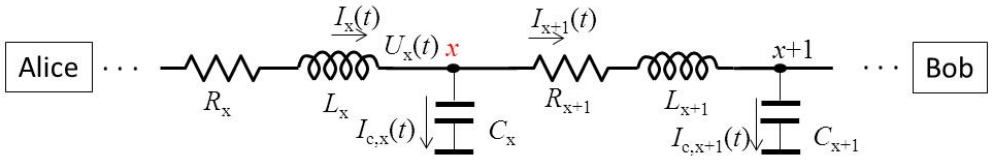

Figure 7 Cable model and cable capacitive currents.

3.3 Realization of the Cable Capacitance Attack

The LTSPICE was used to emulate the practical KLJN system with the RG58 coaxial cable from its library. Throughout the simulations, we assumed that Alice selected R_{L} = 1 kΩ and Bob R_{H} = 9 kΩ; see Figure 8.

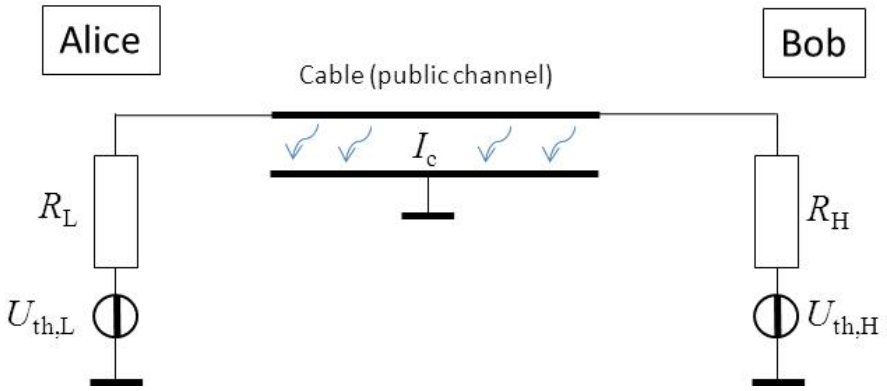

Figure 8 The simulated KLJN system with capacitive current I_{c}. The generator voltages, $U_{\mathrm{th,L}}$ and $U_{\mathrm{th,H}}$, are the Johnson noise voltages of R_{L} and R_{H}, respectively.

3.3.1 Generating the Noise

For the simulations, we generated Gaussian band-limited white noises. According to Johnson's noise formula, the required rms noise voltage U_{th} is

$$U_{\mathrm{th}} = \sqrt{4kT_{\mathrm{eff}}RB_{\mathrm{noise}}}\ . \tag{16}$$

As the mean value is zero, the rms noise voltages are the same as their standard deviations (denoted as σ_{L} and σ_{H} for $U_{\mathrm{th,L}}$ and $U_{\mathrm{th,H}}$, respectively). Thus

$$U_{\mathrm{th,L}}/U_{\mathrm{th,H}} = \sigma_{\mathrm{L}}/\sigma_{\mathrm{H}} = \sqrt{R_{\mathrm{L}}/R_{\mathrm{H}}}\,, \tag{17}$$

where $\sqrt{R_{\mathrm{L}}/R_{\mathrm{H}}} = \sqrt{1/9}$, thus $\sigma_{\mathrm{L}}/\sigma_{\mathrm{H}} = 1/3$. For the simulations, the rms thermal noise voltages of R_{L} and R_{H} were chosen as 1 V and 3 V, respectively, corresponding to $T_{\mathrm{eff}} \approx 7\times10^{16}$ K.

Figure 9a shows the probability density function (histogram) of the noise voltage of R_{L}. In Figure 9b the cumulative distribution as normal probability plot can be seen where a straight line indicates exact normal distribution.

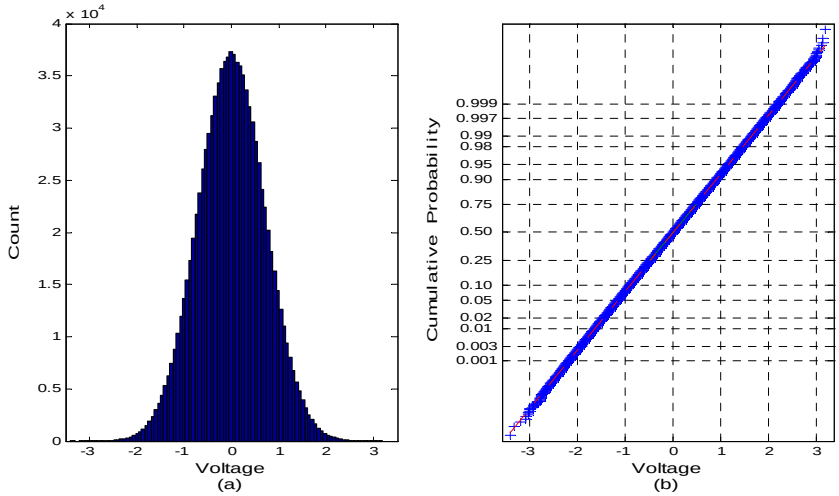

Figure 9 Statistics of the Johnson noise voltage of R_{L} with 10^6 samples. (a) Probability density function (histogram); (b) Cumulative distribution as normal probability plot.

3.3.2 Comparing the Lumped and Distributed Element Models at Different Wavelengths

First, for enhanced computational speed, we explored the possibility of using a lumped element cable model for the simulations because the continuum model simulations are at least 1000 times slower. Our data below proves that lumped elements can be used for high-accuracy simulations at the operational conditions of KLJN.

The quasi-static condition is required for the security of the KLJN system [9,28]. That means

$$D \ll \lambda = v_c / B_{noise} \text{ or } \gamma = \lambda / D \gg 1, \tag{18}$$

where D is the cable length, λ is the shortest wavelength at the highest frequency component of the noise bandwidth B_{noise}, v_c is the propagation velocity in the cable, and γ is the ratio of the wavelength to the cable length. It has been assumed that γ must be at least around 10 to fulfill the KLJN conditions [23-26,28] (*i.e.*, approximate quasi-static electrodynamics; see [23,24] concerning the proof that there are no waves in this limit).

Figure 10a and 10b show the simple lumped element model and the distributed model of the RG58 coaxial cable. Based on the specific inductance and capacitance, the propagation velocity v_c in the RG58 coaxial cable is 2×10^8 m/s. Three simulations were run to compare the resultant voltage waveforms at Alice's side, at three different noise

bandwidths B_{noise} (250 kHz, 25 kHz, 0.25 kHz) on these 2 models. The cable length was set at 1000 m, and based on Eq. 18, the three corresponding wavelengths (λ) were 800 m, 8 km, and 800 km, while the corresponding γ ratios were 0.8, 8 and 800. Other parameters such as the component values of the models used in the simulations are also shown in Figure 10.

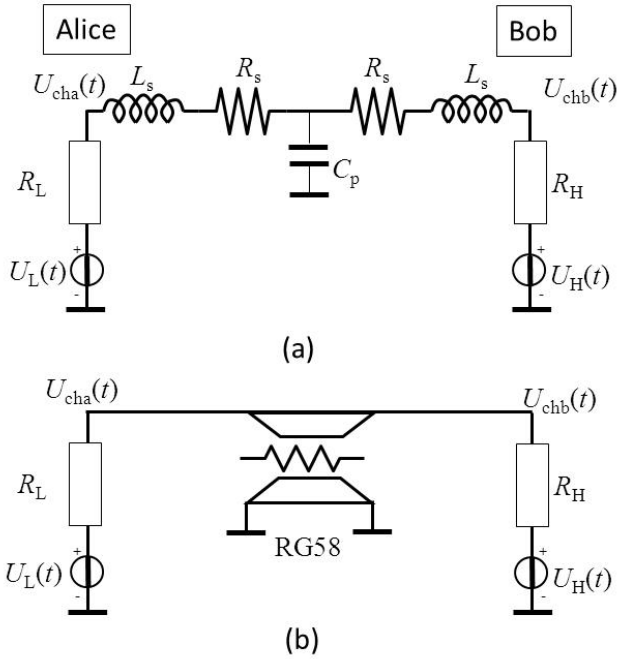

Figure 10 The RG58 coaxial cable models (1000 m length) with R_{L} (1 kΩ) and R_{H} (9 kΩ). The lumped element model: component values $R_{\text{s}} = 10.5\,\Omega$, $L_{\text{s}} = 125\,\mu\text{H}$, $C_{\text{p}} = 100\,\text{nF}$. The distributed model had the following parameters: $R = 0.021\,\Omega/\text{m}$, $L = 250\,\text{nH/m}$, $C = 100\,\text{pF/m}$. The characteristic impedance of the cable is 50 Ω.

Figure 11 shows the simulation results, where $U_{\text{cha,lump}}$ and $U_{\text{cha,dist}}$ are the voltage time functions of the lumped and distributed element models, respectively. In Figure 11a, the two waveforms are significantly different for the shortest wavelength with $\gamma = 0.8$. In such a case, the waves can only be simulated with the distributed model. However, this situation is irrelevant for the operation of KLJN, as mentioned above.

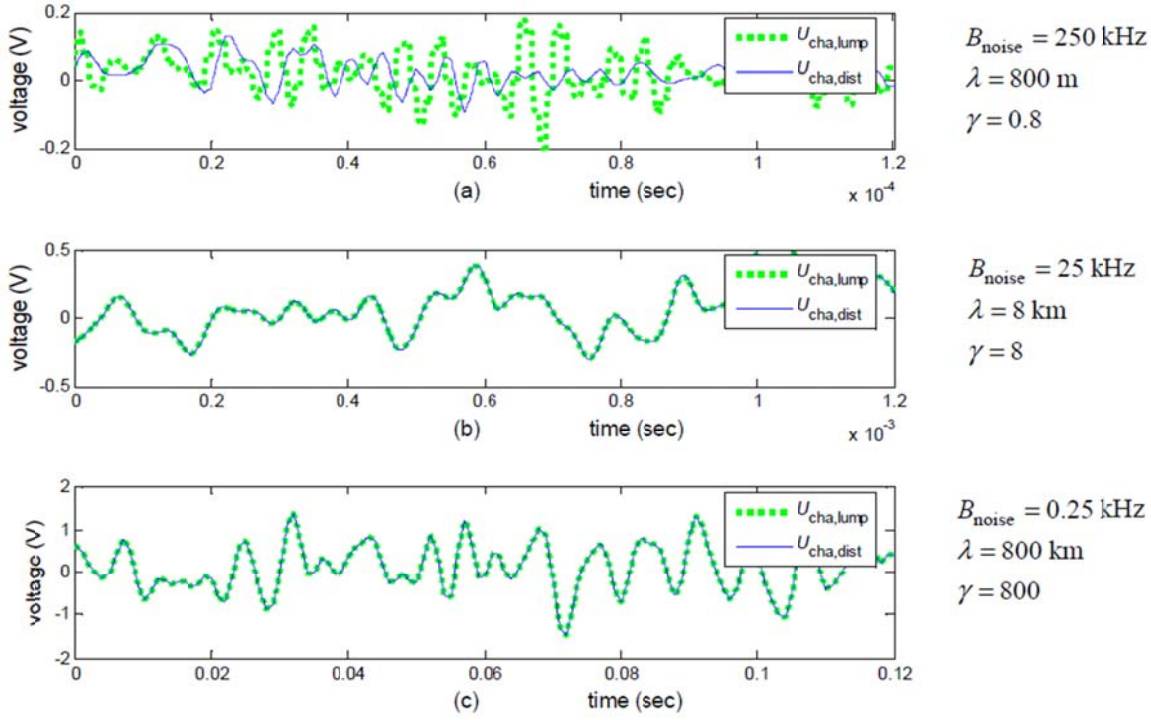

Figure 11 The voltage waveforms at Alice's side, $U_{\text{cha,lump}}$ and $U_{\text{cha,dist}}$, for the lumped and distributed element models, respectively, for a 1000 m cable, at (a) γ = 0.8; (b) γ = 8; (c) γ = 800.

In Figure 11b, with γ = 8, the two waveforms are very similar whereas in Figure 11c, at $\gamma = 800$, the two waveforms are indistinguishable. Thus we can conclude that for

situations $\gamma \geq 8$, the lumped element simulations are satisfactory. Both cases are fine for the KLJN operation and we will use the $\gamma \geq 800$ condition in the rest of the paper.

For our resistor values R_{L} = 1 kΩ and R_{H} = 9 kΩ, the cut-off frequency by the cable capacitance is 1.76 kHz and 17.6 kHz for a 1000 m and a 100 m cable, respectively. To avoid having the cable capacitance truncate the effective bandwidth of the noise, we used noise bandwidth $B_{\mathrm{noise}} = 0.25$ kHz for the noise generators ($\gamma = 800$ at 1000 m and $\gamma = 8000$ at 100 m).

3.3.3 The Attack Protocol

In this section, we discuss the information leak caused by the cable capacitance and evaluate Eve's success probability in terms of guessing the key bits. The fixed bit arrangement is used between Alice and Bob.

During the exchange of the *i*-th bit, Eve measures the cross-correlations:

$$\rho_i^{\mathrm{a}} = \left\langle I_{\mathrm{cha}}(t) \cdot \frac{dU_{\mathrm{cha}}(t)}{dt} \right\rangle_{\tau} , \tag{19}$$

$$\rho_i^{\mathrm{b}} = \left\langle I_{\mathrm{chb}}(t) \cdot \frac{dU_{\mathrm{chb}}(t)}{dt} \right\rangle_{\tau} , \tag{20}$$

where $U_{\text{cha}}(t)$, $I_{\text{cha}}(t)$, $U_{\text{chb}}(t)$ and $I_{\text{chb}}(t)$ are the channel voltages and currents at Alice's and Bob's ends, respectively, see Figure 12. The time average $\langle\ \rangle_{\tau}$ is taken over the bit exchange period τ. Eve calculates $\rho_i = \rho_i^{\text{a}} - \rho_i^{\text{b}}$ $(i = 1,...,N)$ and decides as follows:

$$\begin{array}{l} \text{If} \quad \rho_i > 0 \quad \text{then} \ q_i = 1 \quad (\textit{Eve guessed the bit correctly}). \\ \text{If} \quad \rho_i < 0 \quad \text{then} \ q_i = 0 \quad (\textit{Eve guessed the bit wrongly}). \end{array} \tag{21}$$

When N approaches infinity, the probability of Eve's successful guessing of the bits is equal to the expected value of q and

$$\langle q_i \rangle_N = p_{\text{E}} = 0.5 + \varepsilon, \text{ where } 0 \le \varepsilon < 0.5, \tag{22}$$

where non-zero ε represents an information leak. When $\varepsilon = 0$, the KLJN key exchange system is perfectly secure. We found that the higher the difference between the resistances, the higher the bandwidth, or the higher the parasitic capacitance (the longer the cable), the greater the leak.

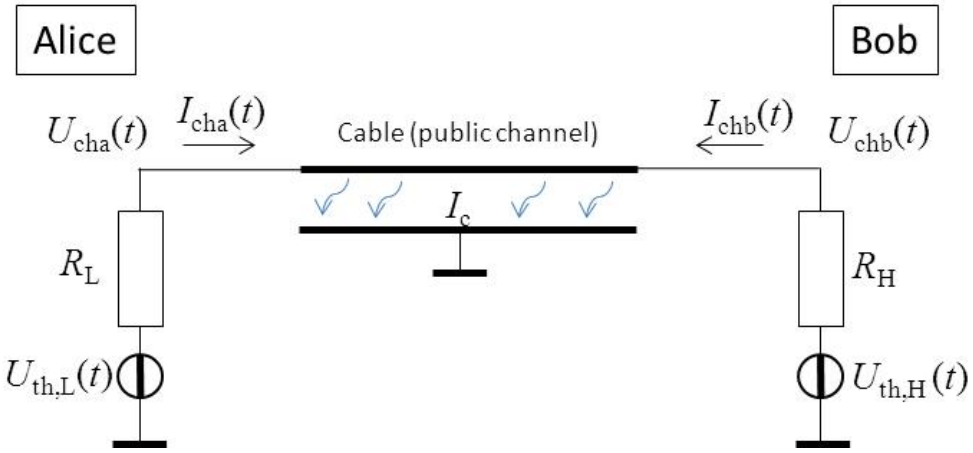

Figure 12 The simulated model with LH bit arrangement (R_L = 1 kΩ and R_H = 9 kΩ). $U_{cha}(t)$, $I_{cha}(t)$, $U_{chb}(t)$ and $I_{chb}(t)$ are the voltages and currents at Alice's and Bob's ends, respectively.

3.3.4 Simulation Results of the Cable Capacitance Attack

We simulated 6 different attack scenarios with these parameters: R_L = 1 kΩ, R_H = 9 kΩ, noise bandwidth B_{noise} = 0.25 kHz, sampling period t_s = 1 msec, for 3 different single-bit exchange durations (measured by the unit of the autocorrelation time of the noise), 20, 50, and 100; at 2 different cable lengths, 100 and 1000 m. At each scenario, the key was 1000 bits long.

The simulation results are shown in Table 2. At bit exchange duration = 20 (50 bits per second), with a 100 m cable, Eve's success probability was 0.509. However, when the cable length was increased to 1000 m with the other parameters unchanged, Eve's success probability increased to 0.622.

Table 2 Attack simulation results—Eve's success probability, p_E , with 1000 bits key length.

Bit Exchange Duration	Bits Per Second	100 m Cable	1000 m Cable
20	50	0.509	0.622
50	20	0.521	0.697
100	10	0.526	0.769

When the bit exchange duration was increased to 50 and 100, Eve's success probability increased accordingly as shown in Table 2. In the most effective attack case, Eve success probability was 0.769.

3.4 Defense against the Attack

3.4.1 Capacitor Killer

The parasitic capacitance of the RG58 coaxial cable can be eliminated by the well-known capacitance compensation technique, called capacitor killer arrangement [17], providing the same voltage on the outer shield of the cable as on the inner wire. This can be done by an ideal voltage follower, see Figure 13. There is no capacitive current from the inner wire to the outer shield, so the attack is nullified.

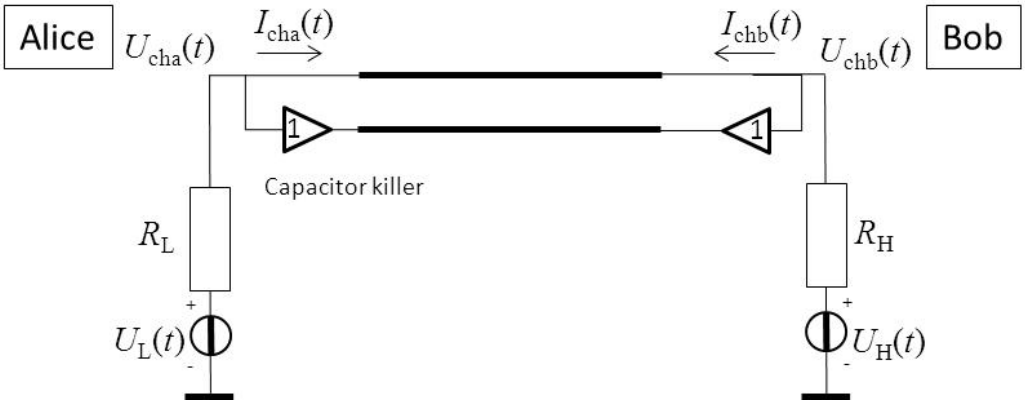

Figure 13 The KLJN system with the capacitor killer. An ideal voltage follower is driving the outer shield, which is not grounded at this time.

We simulated the capacitor killer arrangement in the most effective attack scenario (*i.e.*, when Eve success probability was 0.769). The simulation results showed that Eve's success probability was reduced from 0.769 to 0.501. This indicated that the capacitor killer is very effective in eliminating the leak due to the parasitic capacitance under the practical cable conditions we tested.

3.4.2 Privacy Amplification

Another method to secure the key exchange and to reduce information leak is by utilizing privacy amplification [43]. Due to the extraordinarily low bit error probability of the KLJN system [38-40], privacy amplification (which is basically an error enhancer) can be used to effectively reduce any information leak. The simplest and most secure concept [43] is that Alice and Bob XOR the subsequent pairs of the key bits (*i.e.*, XOR the first and the second bits to get the first bit of the new key, XOR the third and the

fourth bits to get the next one, *etc.*). In this way, the length of the new key will be half of the original one but Eve's success probability will get closer to 0.5; that is, it moves toward the limit of zero information. We simulated the effect of this technique by utilizing the most effective attack scenario (see Table 2). The simulation results showed that by XOR-ing once, Eve's success probability was reduced from 0.769 to 0.642, which was further reduced to 0.544 by XOR-ing a second time to produce a cleaner key with the corresponding significantly higher security and one quarter of its original length.

4. CURRENT INJECTION ATTACK AGAINST THE KLJN SECURE KEY EXCHANGE*

4.1 Introduction

The research in this section is from the paper "Current Injection Attack Against The KLJN Secure Key Exchange", which is submitted to the journal *Metrology and Measurement Systems* and is pending review in 2016.

The current injection attack is an active (invasive) attack, which was introduced in 2006 [9]. Its security analysis was given in 2013 [28], but the attack itself had never been practically tested.

In this section, the attack protocol is proposed. LTSPICE industrial cable and circuit simulator is used to emulate the current injection attack, against the ideal and a practical KLJN system, respectively. The information leak and an eavesdropper's success probability in guessing the exchanged key bits are evaluated. This is followed by the explanation of the defense protocols which can fight against the attacks to eliminate or mitigate the information leak, namely, the instantaneous voltage/current comparison method, and a simple privacy amplification scheme. The defense protocols are also tested and simulation results shown.

---

*Part of this section is a modified version of the paper "Current Injection Attack against the KLJN Secure Key Exchange" by H.P. Chen, M. Mohammad, L.B. Kish, which is submitted to the journal Metrology and Measurement Systems in Feb 2016 and is pending review.

4.2 Current Injection Attack

4.2.1 The Attack Protocol

For the sake of simplicity but without restricting generality, fixed LH bit arrangement with $R_{\mathrm{L}} < R_{\mathrm{H}}$ is assumed. During the exchange of the bit, Eve attempts to identify the location of R_{L} and R_{H} by injecting a Gaussian current $I_{\mathrm{inj}}(t)$ of the same bandwidth as the channel noises into the cable while she measures the following cross-correlations during the exchange of the *i*-th key bit:

$$\rho_i^{\mathrm{a}} = \left\langle I_{\mathrm{inj}}(t) I_{\mathrm{cha}}(t) \right\rangle_{\tau} , \tag{23}$$

$$\rho_i^{\mathrm{b}} = \left\langle I_{\mathrm{inj}}(t) I_{\mathrm{chb}}(t) \right\rangle_{\tau} , \tag{24}$$

where $I_{\mathrm{cha}}(t)$ and $I_{\mathrm{chb}}(t)$ are the channel currents at Alice's and Bob's ends, respectively, see Figure 14. The time average $\langle\ \rangle_{\tau}$ is taken over the bit exchange period τ. According to the current divider rule, a greater current flows to the direction of the lower resistance. With Alice connecting to R_{L} and Bob connecting to R_{H}, the cross-correlation ρ_i^{a} at Alice's side is greater than the cross-correlation ρ_i^{b} at Bob's side. For N bits, Eve calculates $\rho_i = \rho_i^{\mathrm{a}} - \rho_i^{\mathrm{b}}$ $(i = 1,...,N)$ and decides as follows:

If $\rho_i > 0$ then LH (*Eve guessed the bit correctly*), set $q_i = 1$. (25)

If $\rho_i < 0$ then HL (*Eve guessed the bit incorrectly*), set $q_i = 0$. (26)

When N approaches infinity, the probability p_{E} of Eve's successful guessing of the bits converges to the expected value of q and

$$\langle q_i \rangle_N = p_{\mathrm{E}} \text{ where } 0.5 \le p_{\mathrm{E}} \le 1 . \quad (27)$$

The case $p_{\mathrm{E}} = 0.5$, indicates perfect security, that is, Eve's information is zero (equivalent to guessing the key bits by tossing an unbiased random coin [43]).

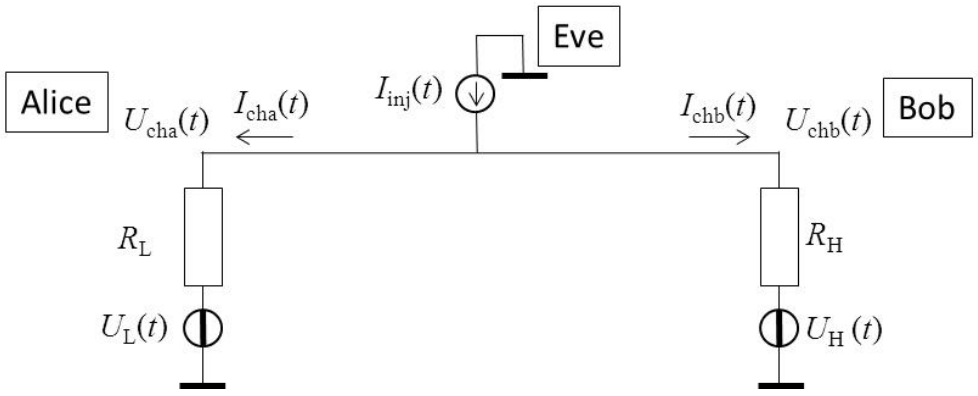

Figure 14 Current injection attack against the ideal KLJN system [9]. $I_{\mathrm{inj}}(t)$ is the injection current. $I_{\mathrm{cha}}(t)$, $I_{\mathrm{chb}}(t)$, $U_{\mathrm{cha}}(t)$ and $U_{\mathrm{chb}}(t)$ are the channel currents/voltages at Alice's and Bob's ends, respectively. (Note, the positive current directions at the two ends are chosen to follow the directions of the components of Eve's injected positive current).

4.2.2 Generic Defense Protocol

To provide security against the current injection attack, Alice and Bob can act similarly against any active (invasive) attacks by measuring the instantaneous voltage and current amplitudes at their ends and compare them via public authenticated data exchange [1,10], see Figure 15. In the case of deviance, Alice and Bob discard the bit or use a more advanced security protocol [1].

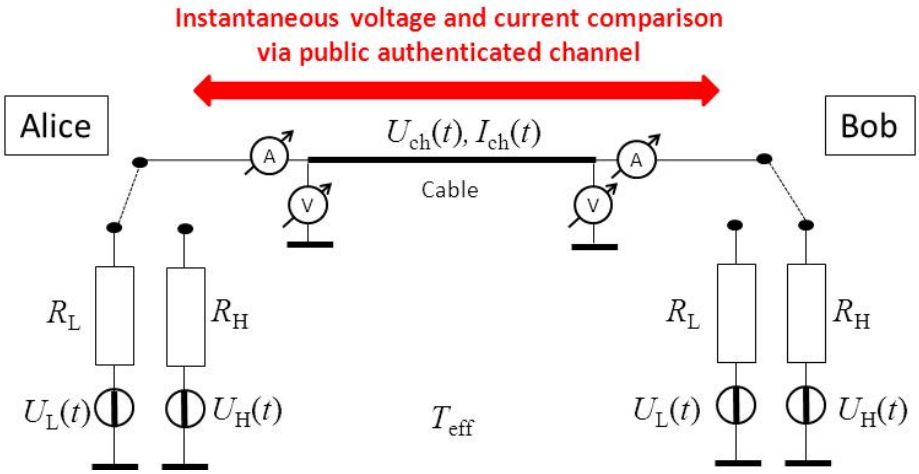

Figure 15 The defense against the current injection attack.

4.3 Simulation Results of the Current Injection Attack

We used the RG58 coaxial cable model from the library of the cable and circuit simulator LTSPICE (Linear Technology), to test both the ideal and a practical KLJN system. We assumed that Alice and Bob selected $R_L = 1\,\mathrm{k\Omega}$ and $R_H = 9\,\mathrm{k\Omega}$,

respectively; the bit exchange period τ was 0.1 s; N=10000; $T_{\text{eff}} = 7.25 \cdot 10^{16}$ K ; and the bandwidth of the Gaussian noises 250 Hz.

We tested three levels of the injected Gaussian current noise, i.e., 0.1%, 1% and 10% of the rms channel current, in four different versions of the KLJN system (see Figure 16). At each scenario, Eve's probability of guessing the bits was calculated, see Table 3.

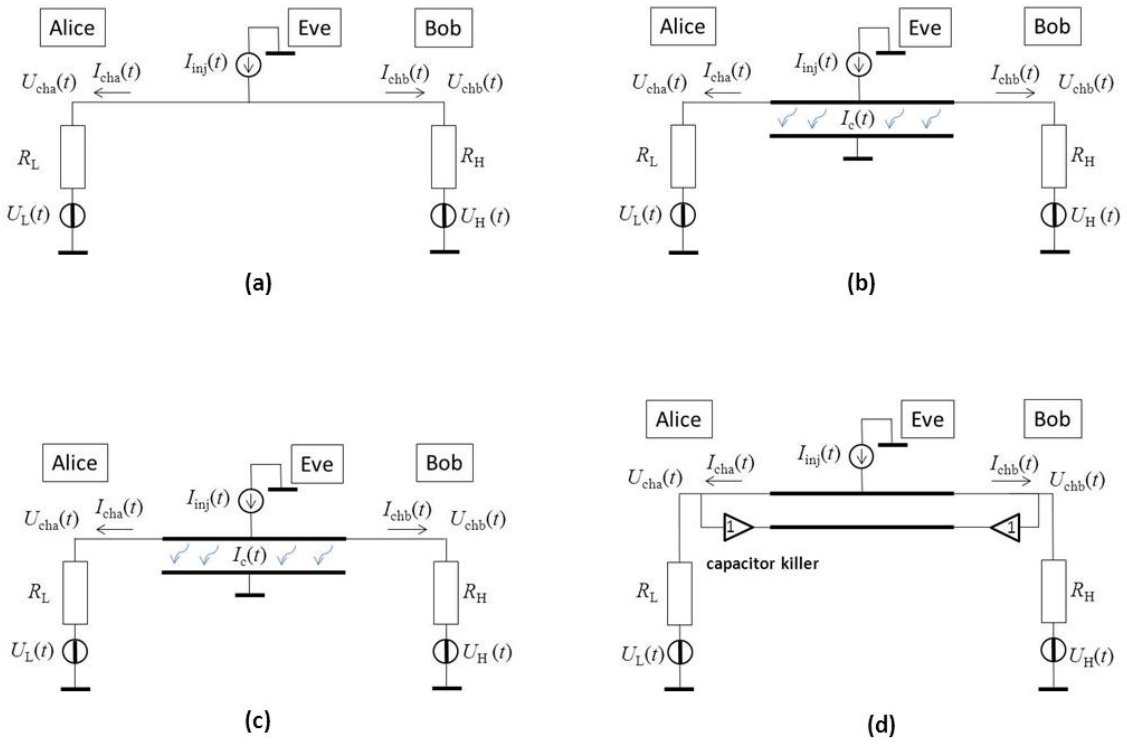

Figure 16 The four different versions of the KLJN system under the current injection attack. (a) the ideal KLJN system; (b) the practical KLJN system with 100 m cable; (c) the practical KLJN system with 1000 m cable; (d) the practical KLJN system with 1000 m cable and capacitor killer (ideal unity-gain voltage buffer) [13]. I_c is the capacitive current from the inner conductor to the outer shield of the cable. The cable is the RG58 coaxial cable.

At 0.1% injected current level, in the ideal KLJN system, p_E was 0.503, which is near to ideal. At 1% and 10% the information leak progressively increased with higher p_E values (0.513 and 0.613). Eve's success probability values in the practical cable-based systems were very similar, see Table 3. Injecting even higher levels of current is also possible but that makes the detection of eavesdropping easier.

Table 3 Eve's success probability, p_E, with 10000 bits key length.

Injection current (in % of the rms channel current)	**0.1%**	**1%**	**10%**
Ideal cable	0.503	0.513	0.613
100 meters cable	0.503	0.513	0.613
1000 meters cable	0.501	0.510	0.608
1000 meters cable with capacitor killer	0.503	0.513	0.613

4.4 Simulation Results of the Defense Methods

4.4.1 The Defense Protocols

As mentioned above, in the ideal KLJN system, Alice and Bob can easily discover the current injection attack by comparing the instantaneous current data [9]. If the currents are different, Alice and Bob can discard the bit.

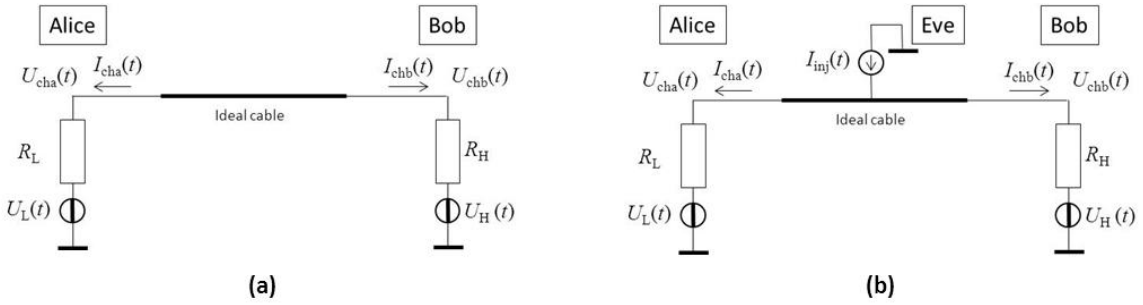

Figure 17 Instantaneous voltage and current comparison against the current injection attack in the ideal KLJN system. (a) No attack. (b) Under current injection attack.

However, in practical systems, the currents are slightly different due to the cable's capacitive current leak. Then Alice and Bob must also monitor and exchange the instantaneous voltage data, too. Then, they input the voltage data into the accurate cable model and compare the simulated currents $I^*_{\text{cha}}(t)$ and $I^*_{\text{chb}}(t)$ with the corresponding measured currents $I_{\text{cha}}(t)$ and $I_{\text{chb}}(t)$, see Figure 18.

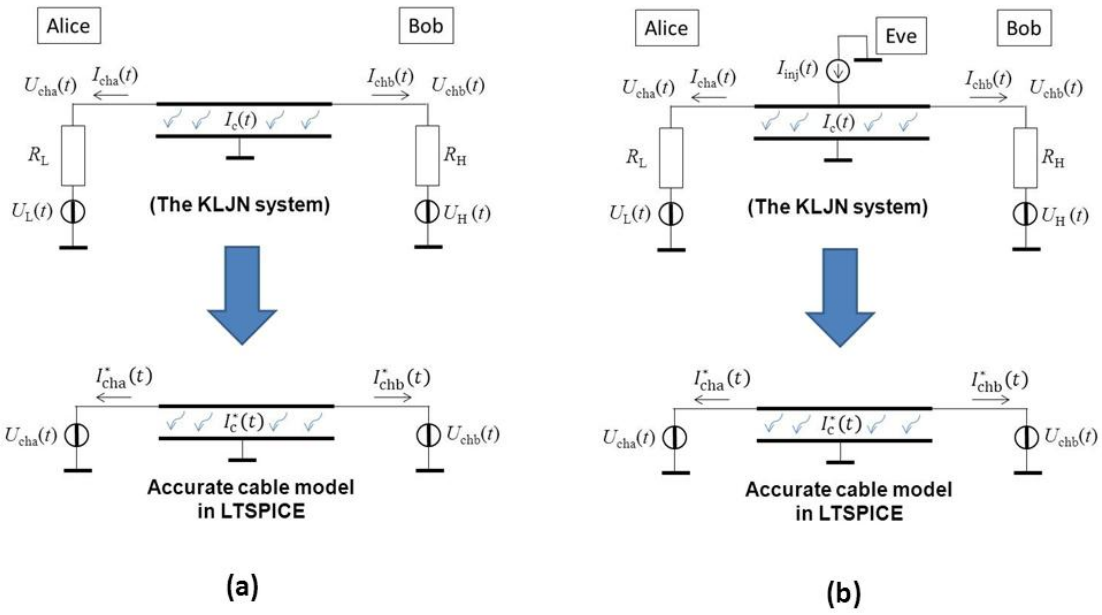

Figure 18 The instantaneous voltage and current comparison against the current injection attack in the practical KLJN system: (a) No current injection attack, (b) Under current injection attack. $I^*_{\text{cha}}(t)$ and $I^*_{\text{chb}}(t)$ are the simulated currents at Alice's and Bob's side, respectively. $I_{\text{c}}(t)$ is the leakage current through the cable parasitic capacitance.

If the measured and the simulated currents are the same,

$$I_{\text{cha}}(t) - I^*_{\text{cha}}(t) = 0, \tag{28}$$

$$I_{\text{chb}}(t) - I^*_{\text{chb}}(t) = 0, \tag{29}$$

then the bit exchange is secure. If the currents are different, an attack may take place. If the difference is greater than a pre-agreed threshold value, Alice and Bob discard the bit.

The simulated comparison results at Alice's side are shown in Figure 19. The solid line indicates a current injection attack and the $I_{\text{cha}}(t)$-$I^{*}_{\text{cha}}(t)$ difference is well visible. Alice and Bob can recognize the attack virtually immediately. The dashed line shows the secure situation with $I_{\text{cha}}(t)=I^{*}_{\text{cha}}(t)$.

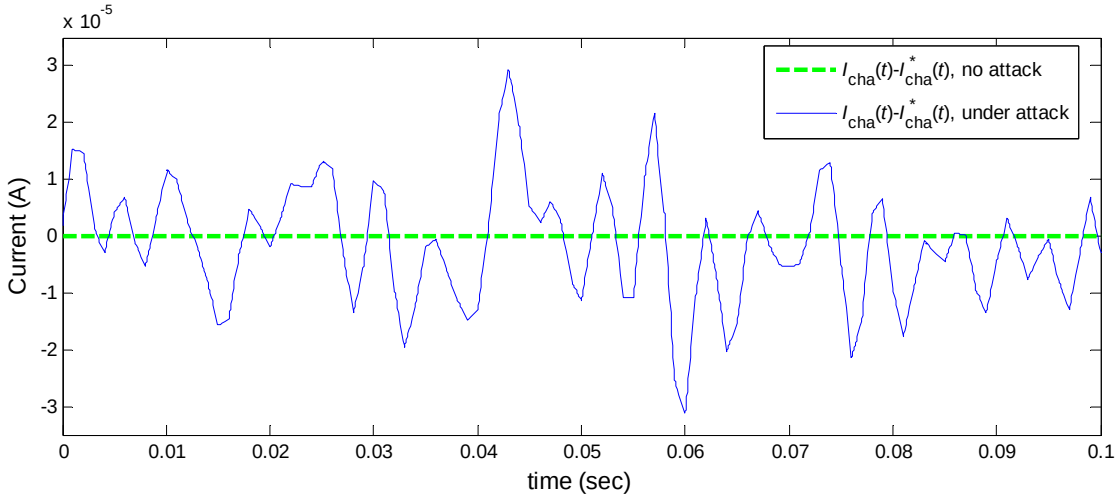

Figure 19 Demonstration of the efficiency of the defense protocol with the practical cable over the bit exchange period. Alice and Bob can recognize the attack virtually immediately. The cable length is 1000 m.

4.4.2 Privacy Amplification

Privacy amplification is a well-known method that can be used to reduce any type of information leak [43]. The KLJN system can reach extraordinarily low bit error probability [38-40]. Thus privacy amplification (which is basically an error enhancer) can be efficiently be used. The simplest technique is the XOR-ing of the subsequent

pairs of the key bits, that is, generating a new key which is cleaner and have half of the length of the original key. We simulated the effect of this technique at the most effective attack scenario, see Table 1. The simulation results showed that by XOR-ing once, Eve's success probability was reduced from 0.613 to 0.530, which was further reduced to 0.502 by XOR-ing the second time. The resulting key length became one quarter of its original length with significantly higher security.

5. CONCLUSIONS*

This section summarizes the main points and the results presented in this dissertation.

In Section 2, the efforts of GAA [22] to utilize time delays in cables to crack the KLJN scheme represent an interesting and novel approach and, as such, deserve attention. However, it should be mentioned that Liu [29] previously used a similar technique, but with unphysical conditions for the simulations [30]. As shown in considerable detail above, GAA's efforts can be irrevocably refuted. It is essential that any attempt to crack the KLJN scheme should be founded on correct physical models.

In Section 3, we have validated the cable capacitance attack by utilizing the LTSPICE simulator. Simulation results show that privacy amplification and/or capacitor killer (capacitance compensation) arrangements can effectively eliminate the leak. In the most effective attack scenario, the capacitor killer arrangement can be used to bring down the eavesdropper's success probability of guessing the bit from 0.769 to 0.501, meaning the eavesdropper has negligible information about the key.

---

*Part of this section is reprinted with permission from "Do Electromagnetic Waves Exist in a Short Cable at Low Frequencies? What does Physics Say?" by H.P. Chen, L.B. Kish, C.G. Granqvist, G. Schmera, 2014. *Fluctuation and Noise Letters*, 13, 1450016, © [2014] by World Scientific Publishing Company.

*Part of this section is reprinted with permission from "Cable Capacitance Attack against the KLJN Secure Key Exchange" by H.P. Chen, E. Gonzalez, Y. Saez, L.B. Kish, 2015. Information, 6, 719-732, © [2015] by Chen, Gonzalez, Saez and Kish.

*Part of this section is a modified version of the paper "Current Injection Attack against the KLJN Secure Key Exchange" by H.P. Chen, M. Mohammad, L.B. Kish, which is submitted to the journal Metrology and Measurement Systems in Feb 2016 and is pending review.

Note that the temperature compensation method [18] based on the non-equilibrium thermodynamical aspects of KLJN to eliminate the information leak in a wire resistance attack does not reduce the efficiency of the cable capacitance attack.

Also, note that there is a new, advanced protocol, the random-resistor-random-temperature (RRRT) KLJN scheme [32], where all the former attacks become invalid or incomplete, and currently no known attack works against it. This is also true for the cable capacitance attack presented above; it is invalid against the RRRT-KLJN scheme. Further studies will be needed to find ways for all the former attack schemes to successfully extract information from the RRRT-KLJN system [32] at non-ideal conditions where they may leak information.

In Section 4, we validated the current injection attack against both the ideal and the practical KLJN system by utilizing LTSPICE. We have shown that the current and voltage comparison method, combined by in-site cable simulations, can efficiently detect and eliminate the attack. In the most effective attack scenario when Eve's success probability was 0.613, privacy amplification technique can effectively bring it down to 0.502 (i.e. Eve can obtain no information). The unconditional security of the practical KLJN key exchange system [1] is preserved against this attack, too.

REFERENCES

1. Kish, L.B.; Granqvist, C.G. On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *Quantum Information Processing* **2014**, *13*, 2213-2219.

2. Cao, X.; Saez, Y.; Pesti, G.; Kish, L.B. On KLJN-based secure key distribution in vehicular communication networks. *Fluctuation and Noise Letters* **2015**, *14*, 1550008.

3. Saez, Y.; Cao, X.; Kish, L.B.; Pesti, G. Securing vehicle communication systems by the KLJN key exchange protocol. *Fluctuation and Noise Letters* **2014**, *13*, 1450020.

4. Gonzalez, E.; Kish, L.B.; Balog, R.S.; Enjeti, P. Information Theoretically Secure, Enhanced Johnson Noise Based Key Distribution over the Smart Grid with Switched Filters. *PloS One* **2013**, *8*, e70206.

5. Gonzalez, E.; Kish, L.B. Key Exchange Trust Evaluation in Peer-to-Peer Sensor Networks with Unconditionally Secure Key Exchange. *arXiv preprint arXiv:1511.06795* **2015**.

6. Kish, L.B.; Kwan, C. Physical unclonable function hardware keys utilizing Kirchhoff-law-Johnson-noise secure key exchange and noise-based logic. *Fluctuation and Noise Letters* **2013**, *12*, 1350018.

7. Kish, L.B.; Saidi, O. Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives. *Fluctuation and Noise Letters* **2008**, *8*, L95-L98.

8. Cho, A. Simple Noise May Stymie Spies Without Quantum Weirdness. *Science* **2005**, *309*, 2148.

9. Kish, L.B. Totally secure classical communication utilizing Johnson-(like) noise and Kirchoff's law. *Physics Letters A* **2006**, *352*, 178-182.

10. Kish, L.B. Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson-(like)-noise cipher and expansion by voltage-based security. *Fluctuation and Noise Letters* **2006**, *6*, L57-L63.

11. Kish, L.B.; Mingesz, R.; Gingl, Z. Unconditionally secure communication via wire. *SPIE Newsroom* **2007**, http://spie.org/x16669.xml.

12. Gingl, Z.; Mingesz, R. Noise properties in the ideal Kirchhoff-law-Johnson-noise secure communication system. *PloS One* **2014**, *9*, e96109.

13. Chen, H.P.; Gonzalez, E.; Saez, Y.; Kish, L.B. Cable Capacitance Attack against the KLJN Secure Key Exchange. *Information* **2015**, *6*, 719-732.

14. Scheuer, J.; Yariv, A. A classical key-distribution system based on Johnson (like) noise---How secure? *Physics Letters A* **2006**, *359*, 737-740.

15. Kish, L.B.; Scheuer, J. Noise in the wire: The real impact of wire resistance for the Johnson(-like) noise based secure communicator. *Physics Letters A* **2010**, *374*, 2140-2142.

16. Kish, L.B. Response to Scheuer–Yariv: "A classical key-distribution system based on Johnson (like) noise—how secure?". *Physics Letters A* **2006**, *359*, 741-744.

17. Mingesz, R.; Gingl, Z.; Kish, L.B. Johnson(-like) Noise Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. *Physics Letters A* **2008**, *372*, 978-984.

18. Kish, L.B.; Granqvist, C.G. Elimination of a Second-Law-Attack, and all cable-resistance-based attacks, in the Kirchhoff-law-Johnson-noise (KLJN) secure key exchange system. *Entropy* **2014**, *16*, 5223-5231.

19. Hao, F. Kish's key exchange scheme is insecure. *IEE Proceedings-Information Security* **2006**, *153*, 141-142.

20. Kish, L.B. Response to Feng Hao's paper "Kish's key exchange scheme is insecure" *Fluctuation and Noise Letters* **2006**, *06*, C37-C41.

21. Vadai, G.; Mingesz, R.; Gingl, Z. Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. *Scientific Reports* **2015**, *5*, 13653.

22. Gunn, L.J.; Allison, A.; Abbott, D. A directional wave measurement attack against the Kish key distribution system. *Scientific Reports* **2014**, *4*, 6461.

23. Chen, H.P.; Kish, L.B.; Granqvist, C.G.; Schmera, G. Do electromagnetic waves exist in a short cable at low frequencies? What does physics say? *Fluctuation and Noise Letters* **2014**, *13*, 1450016.

24. Kish, L.B.; Chen, H.P.; Granqvist, C.G.; Smulko, J. Waves in a short cable at low frequencies, or just hand-waving? What does physics say?, invited paper at the *International Conference on Noise and Fluctuations (ICNF 2015)*, Xi'an, China, in press **2015**.

25. Chen, H.P.; Kish, L.B.; Claes, G.G. On the “Cracking” Scheme in the Paper “A Directional Coupler Attack Against the Kish Key Distribution System” by Gunn, Allison and Abbott. In *Metrology and Measurement Systems* **2014**; Vol. 21, p 389.

26. Kish, L.B.; Gingl, Z.; Mingesz, R.; Vadai, G.; Smulko, J.; Granqvist, C.G. Analysis of an attenuator artifact in an experimental attack by Gunn–Allison–Abbott against the Kirchhoff-law–Johnson-noise (KLJN) secure key exchange system. *Fluctuation and Noise Letters* **2015**, *14*, 1550011.

27. Bennett, C.H.; Jess Riedel, C. On the security of key distribution based on Johnson-Nyquist noise. In *ArXiv e-prints*, **2013**; Vol. 1303, p 7435.

28. Kish, L.B.; Abbott, D.; Granqvist, C.G. Critical analysis of the Bennett-Riedel attack on secure cryptographic key distributions via the Kirchhoff-law-Johnson-noise scheme. *PloS One* **2013**, *8*, e81810.

29. Liu, P.L. A new look at the classical key exchange system based on amplified Johnson noise. *Physics Letters A* **2009**, *373*, 901-904.

30. Kish, L.B.; Horvath, T. Notes on recent approaches concerning the Kirchhoff-law-Johnson-noise-based secure key exchange. *Physics Letters A* **2009**, *373*, 2858-2868.

31. Gunn, L.J.; Allison, A.; Abbott, D. A New Transient Attack on the Kish Key Distribution System. *IEEE Access* **2015**, *3*, 1640-1648.

32. Kish, L.B.; Granqvist, C.G. Random-resistor-random-temperature KLJN key exchange. *arXiv preprint arXiv:1509.08150* **2015**.

33. Mingesz, R.; Kish, L.B.; Gingl, Z.; Granqvist, C.G.; Wen, H.; Peper, F.; Eubanks, T.; Schmera, G. Unconditional security by the laws of classical physics. *Metrology and Measurement Systems* **2013**, *20*, 3-16.

34. Kish, L.B.; Mingesz, R. Totally secure classical networks with multipoint telecloning (teleporation) of classical bits through loops with Johnson-like noise. *Fluctuation and Noise Letters* **2006**, *06*, C9-C21.

35. Kish, L.B. Enhanced Secure Key Exchange Systems Based on the Johnson-Noise Scheme. In *Metrology and Measurement Systems* **2013**; Vol. 20, p 191.

36. Smulko, J. Performance Analysis of the "Intelligent" Kirchhoff-Law–Johnson-Noise Secure Key Exchange. *Fluctuation and Noise Letters* **2014**, *13*, 1450024.

37. Kish, L.B.; Peper, F. Information Networks Secured by the Laws of Physics. *IEICE Transactions on Communications* **2012**, *95*, 1501-1507.

38. Saez, Y.; Kish, L.B.; Mingesz, R.; Gingl, Z.; Granqvist, C.G. Bit errors in the Kirchhoff-Law–Johnson-Noise secure key exchange. *International Journal of Modern Physics: Conference Series* **2014**, *33*, 1460367.

39. Saez, Y.; Kish, L.B. Errors and their mitigation at the Kirchhoff-law-Johnson-noise secure key exchange. *PloS One* **2013**, *8*, e81103.

40. Saez, Y.; Kish, L.B.; Mingesz, R.; Gingl, Z.; Granqvist, C.G. Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange. *J Comput Electron* **2014**, *13*, 271-277.

41. Gonzalez, E.; Balog, R.S.; Kish, L.B. Resource requirements and speed versus geometry of unconditionally secure physical key exchanges. *Entropy* **2015**, *17*, 2010-2024.

42. Kish, L.B.; Granqvist, C.G. Enhanced usage of keys obtained by physical, unconditionally secure distributions. *Fluctuation and Noise Letters* **2015**, *14*, 1550007.

43. Horváth, T.; Kish, L.B.; Scheuer, J. Effective privacy amplification for secure classical communications. *EPL (Europhysics Letters)* **2011**, *94*, 28002.

44. Abbott, D.; Schmera, G. Secure communications using the KLJN scheme. *Scholarpedia* **2013**, *8*, 31157.

45. https://en.wikipedia.org/wiki/Quantum_cryptography

46. Berzanskis, A. Applications of quantum cryptography in government classified, business, and financial communications, *Supercomputing '05*, 12–18 Nov **2005**, Seattle

47. Ursin, R.; Tiefenbacher, F.; Schmitt-Manderbach T.; Weier, H.; Scheidl, T.; Lindenthal, M.; Blauensteiner, B.; Jennewein, T.; Perdigues, J.; Trojek, P.; Ömer, B.; Fürst, M.; Meyenburg, M.; Rarity, J.; Sodnik, Z.; Barbieri, C.; Weinfurter, H.; Zeilinger, A. Entanglement-based quantum communication over 144 km, *Nature Physics* **2007**, 3, pp. 481-186.

48. Bennett, C. H.; Brassard, G.; Breidbart, S.; Wiesner, S. Quantum cryptography, or unforgeable subway tokens, Advances in Cryptology: *Proceedings of Crypto '82*, Plenum Press, Santa Barbara, California, USA, **1982**, pp. 267–275.

49. Yuen, H.P. Essential lack of security proof in quantum key distribution. *arXiv preprint, arXiv:1310.0842* **2013**.

50. Hirota, O. Incompleteness and Limit of Quantum Key Distribution Theory. *arXiv preprint, arXiv:1208.2106* **2012**.

51. Renner, R. Reply to recent skepticism about the foundations of quantum cryptography. *arXiv preprint, arXiv:1209.2423* **2012**.

52. Yuen, H.P. Unconditional Security In Quantum Key Distribution. *arXiv preprint, arXiv:1205.5065* **2012**.

53. Yuen, H.P. On the Foundations of Quantum Key Distribution—Reply to Renner and Beyond. *arXiv preprint, arXiv:1210.2804* **2012**.

54. Yuen, H.P. Security Significance of the Trace Distance Criterion in Quantum Key Distribution. *arXiv preprint, arXiv:1109.2675* **2011**.

55. Yuen, H.P. Key Generation: Foundations and a New Quantum Approach. *arXiv preprint, arXiv:906.5241* **2009**.

56. Merali, Z. Hackers blind quantum cryptographers. *Nature News* **2009**, doi:10.1038/news.2010.436.

57. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications* **2011**, 2, 349, doi:10.1038/ncomms1348.

58. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; Makarov, V.; Kurtsiefer, C. Experimentally Faking the Violation of Bell's Inequalities. *Physical Review Letters* **2011**, 107, doi:10.1103/PhysRevLett.107.170404.

59. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **2010**, 4, 686–689.

60. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Avoiding the blinding attack in QKD. *Nature Photonics* **2010**, 4, doi:10.1038/nphoton.2010.278.

61. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **2010**, 18, 27938–27954.

62. Jain, N.; Wittmann, C.; Lydersen, L.; Wiechers, C.; Elser, D.; Marquardt, C.; Makarov, V.; Leuchs, G. Device Calibration Impacts Security of Quantum Key Distribution. *Physical Review Letters* **2011**, 107, doi:10.1103/ PhysRevLett.107.110501.

63. Lydersen, L.; Jain, N.; Wittmann, C.; Marøy, Ø.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. Superlinear threshold detectors in quantum cryptography. *Physical Review A* **2011**, 84, doi:10.1103/PhysRevA.84.032320.

64. Lydersen, L.; Skaar, J.; Makarov, V. Tailored bright illumination attack on distributed-phase-reference protocols. *Journal of Modern Optics* **2011**, 58, 680–685.

65. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New Journal of Physics* **2011**, 13, doi:10.1088/1367-2630/13/1/013043.

66. Lydersen, L.; Akhlaghi, M.K.; Hamed Majedi, A.; Skaar, J.; Makarov, V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New Journal of Physics* **2011**, 13, doi:10.1088/1367-2630/13/11/113042.

67. Sauge, S.; Lydersen, L.; Anisimov, A.; Skaar, J.; Makarov, V. Controlling an actively-quenched single photon detector with bright light. *Opt. Express* **2011**, 19, doi:10.1364/OE.19.023590.

68. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics* **2009**, 11, doi:10.1088/1367-2630/11/6/065003.

69. Makarov, V.; Skaar, J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Information and Computation* **2008**, 8, 622–635.

70. Lim, C.C.W.; Walenta, N.; Legré, M.; Gisin, N.; Zbinden, H. Random Variation of Detector Efficiency: A Countermeasure Against Detector Blinding Attacks for Quantum Key Distribution. *IEEE J. Sel. Top. Quantum Electron* **2015**, 21, 1–5.

71. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Measurement-device-independent quantum cryptography. *IEEE J. Sel. Top. Quantum Electron* **2015**, 21, 1–11.

72. Jain, N.; Stiller, B.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron* **2015**, 21, 1–10.

73. Sajeed, S.; Chaiwongkhot, P.; Bourgoin, J.P.; Jennewein, T.; Lütkenhaus, N.; Makarov, V. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Physical Review A* **2015**, *91*, doi:10.1103/PhysRevA.91.062301.